JOURNAL OF POLITICAL STABILITY ARCHIVE

Online ISSN: 3006-5879 Print ISSN: 3006-5860
DOI: https://doi.org/10.63468/jpsa.4.1.07
Vol. 4 No. 1 (2026)
https://journalpsa.com.pk/index.php/JPSA/about

Recognized by: Higher Education Commission (HEC), Government of Pakistan

The Role of Cyber Policing in Controlling Dark Web Crimes in Pakistan

Shabana Kausar
Lecturer at Institute of Law University of Sindh Jamshoro

ABSTRACT

The main object of present research is trying to find out solution of presently increasing cyber security issues which are due to rapid expansion of cyberspace which has facilitated an era of digital innovation and connectivity but has also given rise to cybercriminal activities, particularly on the dark web. This study explores the role of cyber policing in combating dark web crimes, emphasizing the evolution of tools, strategies, and collaborative measures employed by law enforcement agencies. Utilizing qualitative research methodologies, this study evaluates the challenges and successes in policing an anonymous and decentralized space. The findings underscore the necessity of international collaboration, advanced technology adoption, and increased public awareness to enhance the effectiveness of cyber policing initiatives. The research contributes to the growing discourse on cybersecurity and the importance of proactive measures to mitigate emerging digital threats. Researcher suggest that cyber police mean such type of software or controlling unit which keep check on online activities of criminals like unusual browsing and dark web activities.

Keywords: Cyber policing, dark web, cybercrime, law enforcement, cybersecurity, cyber threats, illegal marketplaces, cyber laws, digital forensic investigations.

INTRODUCTION

The rapid growth of cyberspace has fostered an era of unprecedented connectivity, but it has also created a shadowy realm where cybercriminals exploit anonymity and evade traditional law enforcement. The dark web, an encrypted part of the internet that conceals users' identities and locations, serves as a haven for illegal activities such as drug trafficking, human trafficking, arms dealing, and cyber fraud. In response, law enforcement agencies globally have adopted cyber policing initiatives to combat these digital threats. This article explores the role of cyber policing in controlling dark web crimes, examining strategies, challenges, and the collaboration required to enforce cybersecurity in an inherently decentralized space.

Cyber Crime investigation techniques

Investigating cybercrime requires a structured approach, combining technical, legal, and procedural expertise. Below is a guide with references to best practices, frameworks, and methodologies:

Initial Response and Incident Handling

Document the complaint or detection of a potential cybercrime. Prioritize the case based on severity and impact. Isolate affected systems to prevent further harm and preserve evidence. (National Institute of Standards and Technology (NIST) Incident Response Guidelines (NIST SP 800-61 Rev. 2).

Legal and Ethical Considerations

Ensure actions align with local, national, and international cybercrime laws (Schneier, B. 2015). Balance evidence collection with privacy rights (e.g., GDPR, HIPAA).(Budapest Convention on Cybercrime (Council of Europe, 2001).

Evidence Collection

Digital Forensics: Acquire data from affected devices using forensically sound methods (e.g., imaging software like EnCase, FTK).Collect data logs (system logs, network traffic, application logs).Preserve metadata to ensure data integrity.

Chain of Custody: Maintain a detailed record of evidence handling to ensure admissibility in court. (SWGDE Best Practices for Digital Evidence Collection).

Technical Investigation: Review server logs, system event logs, and application logs for anomalies. If malware is involved, perform static and dynamic analysis to understand its behavior. Analyze packet captures (e.g., using Wireshark) to identify intrusion points or data exfiltration.

Cryptocurrency Tracking: Trace blockchain transactions related to cybercrimes like ransomware or illicit trading (Casey, E. (2011). *Digital Evidence and Computer Crime)*.

Attribution and Identification: It could be possible by following steps,

i. **IP Tracking:** Use tools to trace IP addresses (e.g., WHOIS, traceroute) while considering proxies or VPNs.
ii. **OSINT (Open Source Intelligence):** Gather publicly available information about suspects using tools like Maltego or Shodan.
iii. **Social Engineering:** Understand behavioral patterns or gain intelligence by infiltrating dark web forums.

Collaboration with Agencies: Collaborate with national and international agencies like FIA and INTERPOL is very much necessary to combat with cyber security breaches. Another way is to contact and seek expertise in analyzing advanced threats. The available labs are Islamabad Forensic Lab, Karachi Forensic Division, FIA Cybercrime wing. Europol's EC3 (European Cybercrime Centre) for international cases. (INTERPOL and UNODC. 2019)

Reporting and Documentation: Prepare a detailed investigation report, including timeline of events, Evidence collected and analysis methods, Findings and conclusions, Recommended actions (ISO/IEC 27043:2015, *Incident Investigation Principles)*.

Prosecution and Legal Proceedings: Work with prosecutors to present evidence effectively in court. Provide expert testimony if required. (Carrier, B. 2005)
Prevention and Mitigation: Complete deep post mortem of incidents are required to identify gaps in security that allowed the incident. (Casey, E. 2011).

LITERATURE REVIEW

Cyber policing has evolved significantly since the internet's inception. In the early days of cyberspace, the concept of cybercrime was minimal, limited to individual hackers who accessed restricted systems for personal gain or curiosity. However, with the expansion of the internet, opportunities for digital crime flourished, creating a need for cyber policing as a specialized domain within law enforcement.

Early Beginnings (1970s-1990s): Cyber policing initially emerged as a response to minor computer-related offenses, such as unauthorized access to systems and data breaches. The 1980s saw the creation of fundamental computer crime laws in the United States, like the Computer Fraud and Abuse Act (CFAA) of 1986, in response to high-profile incidents such as the 1983 hacking of ARPANET, the precursor to the internet.

Formalization and Growth (1990s-2000s): As the internet grew, so did criminal activity within cyberspace, leading to the establishment of dedicated cybercrime units in law enforcement agencies worldwide. Major law enforcement agencies including FIA, FBI, and Interpol during this period started updating and formalizing cyber policing roles to tackle digital fraud, identity theft, and intellectual property theft. The growth of e-commerce in the late 1990s also led to a rise in financial cybercrimes, requiring new strategies for law enforcement (Tavabi, N., Bartley, N., Abeliuk, A., Soni, S., Ferrara, E., & Lerman, K. 2019).

Globalization and Sophistication (2000s-2010s): The early 2000s marked as a period where cyber policing faced enhancing challenges due to the global nature of cybercrime. Criminals leveraged advanced technology, such as encryption and botnets, making it harder for law enforcement to track them. This period saw a collaborative approach to cyber policing with international organizations, including INTERPOL, Europol, and national entities working together to form cross-border cyber task forces (Jalal, R. N. U. D., Alon, I., & Paltrinieri, A. 2021). Operations like the 2013 Operation Onymous, where multiple dark web marketplaces were taken down, marked significant achievements in cyber policing efforts against complex, large-scale cybercrime (Tavabi, N., Bartley, N., Abeliuk, A., Soni, S., Ferrara, E., & Lerman, K. 2019).

Modern Era of Cyber Policing (2010s-Present): With the rise of the dark web, cryptocurrencies, and anonymous networks, cyber policing became more complex. Dark web criminal marketplaces, such as Silk Road and Alpha Bay, posed new challenges, as these platforms enabled illegal trade in drugs, firearms, and stolen data while preserving user anonymity (Chertoff, M. 2017). Modern cyber policing involves advanced tools, such as artificial intelligence, blockchain analysis, and data forensic techniques, to address increasingly sophisticated cybercriminal tactics.

Today, cyber policing continues to evolve, with law enforcement agencies investing in training, technology, and partnerships with tech companies to keep pace with emerging cyber threats.

Dark Web Criminal Activities

The dark web, a hidden part of the internet accessible only through specialized software such as Tor, has become a breeding ground for a variety of illegal activities. Its anonymity and encryption capabilities allow users to interact with minimal risk of detection, which has attracted cybercriminals and illicit enterprises.

The Darkweb, a hidden segment of the deep web, embodies the shadowy and illicit aspects of the internet. Its defining traits include inaccessibility through standard search engines, the need for passwords to gain entry, and concealed user identities, network traffic, IP addresses, and data exchanges (Basheer, R., & Alkhatib, B. 2021). Initially designed for secure military communications and the promotion of free speech, the Darkweb has since been exploited by malicious actors for activities such as extortion, human and child exploitation, illegal trade in contraband and weapons, and the propagation of terrorism and radical ideologies. These actions pose significant threats to societal, communal, and environmental security. Researchers have categorized the Darkweb's primary functions as an e-commerce hub, communication platform, enabler of cybercrimes and untraceable financial transactions, a source of threat intelligence, and a web proxy (Jalal, R. N. U. D., Alon, I., & Paltrinieri, A. 2021).

Two technologies, the Tor network (or Onion routers) and the cryptocurrency Bitcoin, have facilitated the Darkweb's operations by meeting its users' anonymity and untraceable financial transaction requirements. Despite its relatively recent development, with research publications emerging around 2010, the Darkweb's misuse has intensified the challenges of combating crime-as-a-service and advancing cyber threat intelligence. Policy and regulatory complexities make enforcing measures or dismantling Darkweb bridges nearly impossible (Jalal, R. N. U. D., Alon, I., & Paltrinieri, A. 2021). Consequently, research has focused on developing tools and techniques to detect criminal activities and derive cyber threat intelligence from surface web and Darkweb sources. Early efforts included exploratory data analysis to understand Darkweb marketplaces, answering key questions about crime enablers, and developing machine learning and AI-based systems for identifying new malware or exploits with accuracy exceeding 80%.

Recent studies highlight the difficulties faced by law enforcement in identifying potential threats and data breaches on the Darkweb. Innovative approaches, such as using Latent Dirichlet Allocation (LDA) and non-parametric Hidden Markov Models (HMM), have enabled researchers to detect anomalous behaviors, identify trending topics, and anticipate changes tied to unique events. While identifying perpetrators is vital, efforts to apply authorship verification and identification techniques have faced challenges due to the multilingual, mixed-style, and covert nature of communication on the Darkweb (Chertoff, M. 2017).

The COVID-19 pandemic exacerbated Darkweb activities, as widespread fear and lockdowns drove increased demand for illicit goods and services. The pandemic saw a rise in illegal vaccine trade, counterfeit vaccination certificates, and readily available medications on the Darkweb, posing public health risks (Levi, M., & Williams, M. 2013). Reports suggest the pandemic also intensified detrimental behaviors such as loneliness and gambling, linked to increased Darkweb usage. Additionally, hoarding addictive drugs, driven by fears of shortages, emerged as a significant issue during this period.

The Darkweb's operations starkly oppose the United Nations' Sustainable Development Goals (SDGs), which purpose is to eradicate poverty, ensure well-being, and promote peace and sustainability (Chertoff, M. 2017). Activities on the Darkweb, such as cybercrime, illegal trade, and misinformation dissemination, undermine efforts toward SDG objectives, including poverty alleviation (SDG 1), hunger eradication (SDG 2), good health and well-being (SDG 3), quality education (SDG 4), and peace, justice, and strong institutions (SDG 16). Research into the Darkweb's societal impact is vital for addressing these challenges.

This study identifies four key contributions to advancing Darkweb research. First, it provides a bibliometric analysis of 1,068 publications from 2012 to 2022, including the pandemic's critical influence on Darkweb usage by legitimate and illegitimate actors. Second, it maps thematic research areas using science mapping techniques. Third, it uniquely explores the direct alignment between Darkweb research and SDGs. Lastly, it identifies underexplored topics and suggests future research directions to address gaps in understanding the Darkweb's multifaceted impacts.

Dark Web is a place were extremely psychopath individuals and criminals do there dirty activities and they offer whatever they want for example drugs, weapons, sexually explicit materials, even human organs, human meat, human children to satisfy their criminal and sinner clients. Now a days these activities are started growing everywhere even in Pakistan many journalist are working and disclosing unbelievable facts (Bergeron, A., Décary-Hétu, D., Giommoni, L., & Villeneuve-Dubuc, M. P. 2022)..

Drug Trafficking

One of the primary activities on the dark web involves the trade of illegal drugs. Sites like Silk Road and, later, Alpha Bay served as large-scale drug marketplaces, where buyers and sellers could conduct transactions with relative anonymity(Levi, M., & Williams, M. 2013). Law enforcement takedowns of these sites highlighted the extensive trade in controlled substances facilitated by the dark web.

Weapons and Explosives Trade

The dark web hosts marketplaces where firearms, explosives, and other weapons are sold. These transactions typically occur in untraceable cryptocurrencies, making it difficult for authorities to monitor and control arms trafficking effectively.

Human Trafficking and Exploitation

Human trafficking, including sex trafficking, is an ongoing issue on the dark web. While this activity is challenging to trace and verify, law enforcement has identified forums and chat rooms that facilitate the illegal sale of human services and exploitation.

Financial Fraud and Identity Theft

The dark web contains numerous forums and sites dedicated to financial crimes, including the sale of stolen credit card information, bank account details, and identity documents. Criminals often use "carding" forums to buy and sell personal data for fraudulent financial activities.

Cyber Weapons and Hacking Services

The dark web is a marketplace for hacking tools, malware, and cyberattack services, including Distributed Denial of Service (DDoS) attacks, ransomware, and custom-built malware. Some dark web vendors even offer hacking-for-hire services to interested clients, providing them with tailored cyberattacks against individuals, organizations, or government entities (Levi, M., & Williams, M. 2013).

Counterfeit Goods and Documents

The trade in counterfeit goods, including passports, driver's licenses, and counterfeit money, has thrived on the dark web. These goods cater to criminals seeking to establish false identities and avoid detection by authorities.

Child Exploitation and Abuse Material (CEAM)

One of the most disturbing aspects of dark web criminal activity involves the sharing and distribution of child exploitation materials. Law enforcement agencies have focused substantial efforts on eradicating CEAM networks on the dark web, with successful operations leading to arrests and site shutdowns.

Terrorism and Extremist Networks

Terrorist organizations and extremist groups use the dark web to spread propaganda, recruit members, and coordinate operations. By leveraging anonymity, these groups can communicate and mobilize without exposure to public scrutiny or monitoring by intelligence agencies (Levi, M., & Williams, M. 2013). Law enforcement faces immense challenges in combating these dark web crimes due to the encryption, anonymity, and international jurisdictional issues. Efforts to tackle dark web crime often involve sophisticated cyber policing tactics, inter-agency collaborations, and extensive international cooperation.

Problem statement

Increasing dark web activities in Pakistan are an open challenge for society and internet users. Researcher identified that still law enforcement agencies remain failed even in tracing out these activities. Present research is done to highlight this issue and propose some solutions.

RESEARCH METHODOLOGY

Researcher relied on secondary data and employed qualitative method of research to complete present article. All results and discussion are done in

descriptive format.

Cyber Policing Tools and Techniques

Cyber policing has evolved to use advanced tools and techniques to monitor, investigate, and prosecute cybercriminals who operate both on the open internet and the dark web (Levi, M., & Williams, M. 2013). Due to anonymity in online world and distance from real world internet users and cyber criminals feel false sense of security and did not afraid from repeating crime patterns. Crime patterns and its repetition can help to work any computer program or AI based module of cyber police which can remain active all time and control Dark web activities of criminals. Given the anonymity and encryption used by cybercriminals, cyber policing agencies need specialized resources to stay one step ahead. Here's a detailed look at the major tools and techniques used in modern cyber policing.

1. Digital Forensic Analysis:

- **Disk Imaging and Data Recovery**: Forensic specialists use tools like EnCase and FTK Imager to create exact copies of digital storage devices and recover deleted or hidden data. This allows investigators to analyze hard drives, USBs, and other storage media for evidence without altering the original data.
- **Memory Analysis**: Tools like Volatility help extract and analyze data from a computer's volatile memory (RAM), which can reveal passwords, IP addresses, and other useful information about recent activity.
- **Network Forensics**: Monitoring network traffic and logging data can provide insights into suspicious behaviors and unauthorized access. Tools like Wireshark capture and analyze data packets to identify unusual traffic patterns and potentially malicious connections.
- **Timeline Analysis**: Forensic investigators create chronological sequences of system events and user activities to understand the sequence of events during a cybercrime.

2. De-Anonymization Techniques

- **Traffic Analysis**: Law enforcement agencies use traffic correlation techniques to identify patterns in encrypted communication. By monitoring data entering and exiting the Tor network, for instance, they can potentially link a user's entry and exit points, helping to identify individuals behind anonymous accounts (Levi, M., & Williams, M. 2013).
- **Browser Fingerprinting**: Cyber policing can identify unique attributes of browsers, such as installed plugins, screen resolution, and language settings. These "fingerprints" can help track and profile users, even when using anonymized networks.
- **User Behavioral Analysis**: User activities, like login patterns and typing rhythms, are monitored to identify and match a user's digital footprint across different sites, even if they attempt to anonymize themselves.

3. Artificial Intelligence (AI) and Machine Learning (ML)

- **Pattern Recognition**: AI can detect patterns that indicate cybercrime activity,

such as the repetitive purchasing of illicit goods or usage of similar transaction keywords across dark web marketplaces. Machine learning algorithms analyze these patterns to alert law enforcement to suspicious activities.

- **Sentiment Analysis and Text Mining**: NLP-based techniques allow law enforcement to monitor forums, social media, and dark web marketplaces. Sentiment analysis identifies threats, while text mining categorizes and identifies suspicious keywords related to criminal activities.
- **Image and Video Analysis**: AI tools can process large volumes of images and video to detect illegal content, like counterfeit goods or child exploitation materials. Machine learning models can assist in identifying objects, faces, and locations in multimedia content.

4. Blockchain Analysis for Cryptocurrency Tracking

- **Address Clustering**: Blockchain forensics tools like Chain analysis and Elliptic use clustering algorithms to group related cryptocurrency addresses. By identifying clusters associated with dark web transactions, cyber police can trace transactions to specific entities.
- **Transaction Graphs**: Blockchain analysis tools create visual transaction graphs that help trace the flow of funds. This can identify patterns in laundering activities, such as "peel chains," where illicit funds are split and distributed to multiple addresses.
- **Wallet Monitoring**: Law enforcement agencies monitor high-risk cryptocurrency wallets associated with dark web markets, ransomware payments, or known criminal entities. Alerts are generated for suspicious transactions that might indicate active criminal activity.

5. OSINT (Open-Source Intelligence) Gathering

- **Social Media Monitoring**: Platforms like Facebook, Twitter, and specialized forums often serve as data sources for cyber policing. Monitoring social media profiles and posts can provide valuable leads on cybercriminal networks (Levi, M., & Williams, M. 2013).
- **Search Engines and Metadata Analysis**: OSINT tools like Maltego and Shodan allow cyber police to analyze metadata, discover connections between entities, and locate exposed devices and vulnerable systems.
- **Dark Web Crawlers**: Tools like Hunchly and Memex, created for law enforcement, assist in indexing dark web content. These crawlers systematically collect data from dark web forums, marketplaces, and private networks to identify illicit activity and track criminal trends.

6. Network Analysis Tools

- **Packet Capture and Analysis**: Network monitoring tools such as Wireshark and TCPdump allow law enforcement to analyze data packets flowing through a network. They help trace IP addresses and detect intrusion attempts, data exfiltration, and unusual network traffic patterns.
- **Deep Packet Inspection (DPI)**: DPI examines packet contents beyond just header information. By examining the data payload, it can identify encrypted malware

signatures or banned content, making it easier to detect malicious activities in real-time.

- **Anomaly Detection**: Cyber policing uses network behavior analysis tools like Darktrace to detect anomalies in network traffic that may indicate unauthorized access, botnet activity, or data breaches.

7. Undercover Operations and Social Engineering

- **Undercover Profiles**: Law enforcement officers create fake profiles on dark web markets and forums to gain trust and gather evidence. These undercover operations are designed to infiltrate and dismantle criminal networks.
- **Honey Pot and Honey Net Deployment**: Honeypots, or decoy servers, lure cybercriminals into interacting with what they believe to be vulnerable systems. Law enforcement uses these decoys to gather data on attackers, track malicious IP addresses, and understand cybercriminal tactics.
- **Sting Operations**: These operations involve posing as buyers or sellers to gather intelligence on dark web markets. Law enforcement often targets key facilitators in these operations to dismantle the network's hierarchy.

8. Malware Analysis: Static and Dynamic Analysis: Malware analysis tools like IDA Pro and Ghidra allow cyber police to reverse-engineer malware and understand its functions. Static analysis inspects malware code without executing it, while dynamic analysis observes malware behavior during execution.

- **Sandboxing**: Sandboxing tools like Cuckoo Sandbox run malware in isolated environments, allowing investigators to observe behavior without risking real systems. This helps to understand malware capabilities, such as data exfiltration or keylogging functions.
- **Signature-Based Detection**: Cyber police use signature-based detection to match known malware signatures with detected files. Behavioral analysis, meanwhile, identifies malware based on unusual activity patterns.

9. Geolocation and Device Tracking

- **IP Geolocation**: Tools like MaxMind's GeoIP provide approximate geographic locations of IP addresses. This information, combined with other evidence, can help identify criminal hotspots and locate potential suspects.
- **Wireless Tracking**: Law enforcement uses Wi-Fi network data to approximate locations based on nearby signals. This approach can help trace devices or identify connections among devices used in coordinated cybercrime.
- **GPS and Mobile Tracking**: Law enforcement can use mobile tracking technology to trace criminals in real time. With legal permissions, agencies can leverage telecom data to track devices associated with dark web activities or cryptocurrency wallets.

10. Intelligence Sharing Platforms to collaborate:

a. **INTERPOL and Europol Databases**: These international agencies offer intelligence databases and collaboration platforms that help national law enforcement agencies share intelligence and coordinate efforts.
b. **ISACs (Information Sharing and Analysis Centers)**: ISACs for various sectors

(e.g., Financial Services, Healthcare) facilitate information sharing between private companies and law enforcement. These collaborations help prevent and address cyber threats that cross sectors.

c. **Automated Threat Intelligence Platforms**: Threat intelligence feeds from platforms like MISP and Recorded Future provide real-time alerts on cyber threats. These feeds help law enforcement stay updated on emerging threats, tactics, and indicators of compromise.

Challenges in Policing the Dark Web

Policing the dark web presents a unique and complex set of challenges due to its inherent structure and the tools that enable user anonymity and data encryption. One of the primary difficulties lies in the extensive use of anonymizing networks, like Tor, which conceal users' identities and locations by routing traffic through multiple volunteer-operated servers worldwide. This anonymity shields both users and operators of dark web marketplaces, making it difficult for law enforcement to attribute criminal activity to specific individuals. Additionally, the decentralized nature of these networks means there is no central authority or entity to regulate or monitor activities, allowing illegal marketplaces to thrive without oversight. Another significant obstacle is encryption: most dark web platforms use strong end-to-end encryption, meaning that even if law enforcement gains access to a server, the data is often unreadable without encryption keys.

Jurisdictional issues add further complexity, as dark web servers and users are often spread across multiple countries with varying legal standards and cooperation protocols. International collaboration is essential yet challenging, as legal and procedural differences between countries can delay investigations or hinder evidence collection. The dark web also supports transactions in cryptocurrencies, which are difficult to trace and facilitate laundering and the transfer of illicit funds. Additionally, dark web communities are highly adaptive, quickly relocating to new platforms or creating mirror sites when one is shut down, which forces law enforcement agencies into a continuous game of "cat and mouse." The dynamic nature of dark web activities, combined with these technical, legal, and procedural barriers, makes policing the dark web a formidable task that demands constant innovation, cross-border cooperation, and specialized cyber skills within law enforcement.

Dark web crimes and proving it in Court of Law:

Proving crimes committed on the dark web requires a blend of technical expertise, legal compliance, and meticulous investigative methods. Below is a comprehensive approach to proving dark web crimes:

1. Digital Evidence Collection

To prove a crime, collecting digital evidence is the first step:

a. De-Anonymization Techniques: Traffic Analysis: Use correlation techniques to trace communication through anonymizing networks like Tor.

- **Browser Fingerprinting**: Identify users by analyzing browser configurations, plugins, and usage patterns.

- **Behavioral Analysis**: Study user behavior, such as login times and transaction habits, to link activity to individuals.

b. Cryptocurrency Tracking: Blockchain Analysis: Tools like Chain analysis and Elliptic can trace transactions to uncover financial links. Group related cryptocurrency addresses to identify networks of illicit transactions. Police should use law enforcement tools (e.g., Memex or Hunchly) to index and monitor dark web content for illegal activity. **d. Digital Forensics:** Extract data from seized devices using tools like EnCase and FTK Imager. Capture network data to identify communications linked to criminal activity.

2. Building a Chain of Custody: Secure all evidence with proper documentation to ensure admissibility in court. Maintain detailed logs of evidence collection, storage, and analysis.

3. Linking Activity to Individuals: Law enforcement can create undercover profiles to engage with suspects on the dark web. Police should analyze timestamps, IP logs, and device information to tie online actions to suspects. Use geolocation tools and forensic analysis to identify and trace devices used in criminal activity.

4. Legal and Jurisdictional Considerations: To ensure all evidence collection methods comply with legal standards and warrant should be obtained, including search and seizure laws. International Collaboration is necessary, Government must have to take step to work with global agencies (e.g., INTERPOL, Europol) to address jurisdictional challenges.

5. Collaboration with Experts: Partner with cybersecurity firms and technology providers to access advanced tools and expertise. Work with financial institutions to trace financial flows and identify beneficiaries.

6. Identifying and Preserving Online Evidence: For the purpose to prove the crime following steps could be taken to collect the available data:

- **Screenshots and Data Capture**: Secure screenshots, chat logs, and transactional data from dark web marketplaces.
- **Archive Links and Pages**: Use tools to archive web pages for future reference.

7. Use of Advanced Technologies

- **Artificial Intelligence (AI)**: AI-based tools can analyze patterns and detect anomalies in dark web activities.
- **Machine Learning**: Identify recurring trends in illegal activities and predict potential criminal behavior.
- **Deep Learning for Image Recognition**: Use AI to identify illegal materials (e.g., child exploitation images).

8. Expert Testimony: Present expert witnesses who can explain the technical aspects of dark web investigations to the court. Include cybersecurity specialists, blockchain analysts, or forensic experts.

9. Establishing Intent and Motive: Corroborate evidence to demonstrate the suspect's intent to commit a crime. Highlight communications, transactions, or actions that indicate criminal motives.

10. Monitoring Suspects: Use surveillance and intercept communications with

proper legal authorization to gather additional evidence.

Results and Discussion: Results: The study identified significant challenges in policing the dark web, including jurisdictional issues, the pervasive use of anonymizing technologies, and the adaptability of cybercriminal networks (Bergeron, A., Décary-Hétu, D., Giommoni, L., & Villeneuve-Dubuc, M. P. 2022).. Law enforcement agencies struggle with unclear reporting protocols, low public confidence, and a lack of specialized training among officers. The research highlights the following findings:

1. Underreporting of Cybercrimes: Many victims of cybercrimes are reluctant to report incidents, resulting in a significant "dark figure" of unreported cases.
2. Technological Gaps in Law Enforcement: Despite advancements, many officers lack the training and resources necessary to address sophisticated cyber threats effectively.
3. Effective Tools and Techniques: Tools such as blockchain analysis, digital forensics, and artificial intelligence have emerged as critical assets in combating dark web crimes.
4. Collaborative Successes: International operations, such as the takedown of major dark web marketplaces, demonstrate the importance of cross-border collaboration in cyber policing.

DISCUSSION

The findings reveal a complex and evolving landscape of dark web criminal activities that challenge traditional law enforcement methods. The pervasive use of encrypted networks, like Tor, and untraceable cryptocurrencies necessitates adopting innovative approaches such as de-anonymization techniques, AI-driven analysis, and advanced digital forensics. Despite these advancements, the study highlights the pressing need for enhanced training and resources within law enforcement agencies to close the technological gap.

International collaboration remains paramount, as cybercrime transcends national borders. Initiatives such as INTERPOL and Europol's joint efforts underscore the potential for success when countries pool resources and expertise. However, differing legal standards and procedural delays impede timely action.

Finally, the study emphasizes the importance of public awareness and streamlined reporting mechanisms. By addressing these gaps, law enforcement agencies can foster a more robust defense against the rapidly evolving threats posed by dark web crimes.

CONCLUSION

Darkweb activities are increasing day by day and these activities are illegal and providing all facilities and services to criminal. In era of digital technology Cyber policing tools and techniques need to become highly specialized and technologically advanced, reflecting the sophisticated nature of modern cybercrime. Through digital forensics, blockchain analysis, network monitoring, AI, undercover

operations, and international collaboration, cyber policing agencies are better equipped to combat dark web and internet-based criminal activities. However, the rapidly changing technology landscape means that law enforcement agencies must continuously adapt to effectively address the new tactics employed by cybercriminals.

Recommendations/ Suggestions

Researcher advance following recommendations on the base of research:

1. For cyber space monitoring and to control Dark web activities AI based tools and software should be designed and may be recognized by Government after complete satisfaction and examination.
2. System should stay updated on emerging technologies and criminal tactics.
3. Law enforcement agencies should regularly update AI models to handle new threats.
4. All stake holders should Equip law enforcement personnel with skills to interpret AI findings.
5. Provide training to concern department on cybercrime laws, dark web operations, and ethical AI use.
6. Monitor cryptocurrency transactions, often used in dark web deals, by analyzing blockchain activity.
7. Establish transparent policies to ensure AI is not used for mass surveillance or privacy violations.

REFERENCES

Albizri, A., Nehme, A., & Harfouche, A. (2022). A Systematic Review on Using Hacker Forums on the Dark Web for Cyber Threat Intelligence. In *28th Americas Conference on Information Systems, AMCIS 2022* (28th Americas Conference on Information Systems, AMCIS 2022). Association for Information Systems.

Action Fraud. (2020a). *Reporting fraud and cybercrime*. Retrieved from https://www.actionfraud.police.uk/data

Aiken, M., McMahon, C., & O'Neill, L. (2016). The psychology of cybercrime. *Computers in Human Behavior, 59*, 12-20.

Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cybersecurity awareness campaigns: Why do they fail to change behavior? *Cyberpsychology, Behavior, and Social Networking, 22*(8), 675-682.

Ball, H., & Webster, W. (2017). Policing cybercrime: The impact of technology on traditional practices. *Policing and Society, 27*(3), 347-359.

Burruss, G. W., Holt, T. J., & Bossler, A. M. (2019). Law enforcement practices for addressing cybercrime: Perceptions from officers. *Police Quarterly, 22*(4), 434-458.

Button, M., Lewis, C., & Tapley, J. (2020). *Fraud and its victims: Perceptions and attitudes*. Crime and Justice Press.

Basheer, R., & Alkhatib, B. (2021). Threats from the dark: A review over Darkweb investigation research for cyber threat intelligence. *Journal of Computer Networks and Communications.*

Bernaschi, M., Celestini, A., Guarino, S., & Lombardi, F. (2017). Exploring and analyzing the Tor hidden services graph. *ACM Transactions on the Web, 11*(4), 1–26.

Bracci, A., Nadini, M., Aliapoulios, M., McCoy, D., Gray, I., Teytelboym, A., Gallo, A., & Baronchelli, A. (2022). Vaccines and more: The response of Darkweb marketplaces to the ongoing COVID-19 pandemic. *PLoS ONE, 17*(11), e0275288.

Bergeron, A., Décary-Hétu, D., & Giommoni, L. (2020). Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy, 83,* 102870.

Bergeron, A., Décary-Hétu, D., Giommoni, L., & Villeneuve-Dubuc, M. P. (2022). The success rate of online illicit drug transactions during a global pandemic. *International Journal of Drug Policy,*V. *99,p.*103-452.

Bracci, A., Nadini, M., Aliapoulios, M., McCoy, D., Gray, I., Teytelboym, A., Gallo, A., & Baronchelli, A. (2022). Vaccines and more: The response of Darkweb marketplaces to the ongoing COVID-19 pandemic. *PLoS One, 17*(11), e0275288. https://doi.org/10.1371/journal.pone.0275288

Bergeron, A., Décary-Hétu, D., & Giommoni, L. (2020). Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy, 83*, 102870. https://doi.org/10.1016/j.drugpo.2020.102870

Bergeron, A., Décary-Hétu, D., Giommoni, L., & Villeneuve-Dubuc, M. P. (2022). The success rate of online illicit drug transactions during a global pandemic. *International Journal of Drug Policy, 99*, 103452. https://doi.org/10.1016/j.drugpo.2021.103452

Broadhurst, R., Lord, D., Maxim, D., Woodford-Smith, H., Johnston, C., Chung, H. W., & Sabol, B. (2018). Malware trends on 'Darknet' crypto-markets: Research review. *SSRN 3226758.*

Beshiri, A. S., & Susuri, A. (2019). Darkweb and its impact on online anonymity and privacy: A critical analysis and review. *Journal of Computer Communications, 7*(3), 30.

Broadhurst, R., Lord, D., Maxim, D., Woodford-Smith, H., Johnston, C., Chung, H. W., & Sabol, B. (2018). Malware trends on 'darknet' crypto-markets: Research review. Available at SSRN: https://doi.org/10.2139/ssrn.3226758

Chertoff, M. (2017). A public policy perspective of the Darkweb. *Journal of Cyber Policy, 2*(1), 26–38.

Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security, 105*, 102258. https://doi.org/10.1016/j.cose.2021.102258

Chen, H., Chung, W., Qin, J., Reid, E., Sageman, M., & Weimann, G. (2008). Uncovering the Darkweb: A case study of Jihad on the web. *Journal of the*

American Society for Information Science and Technology, 59(8), 1347–1359.
Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. *Computers & Security, 105,* 102258.
Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research, 133,* 285–296.
Europol. (2020). *Internet Organized Crime Threat Assessment (IOCTA)*. Retrieved from [URL Placeholder]
FBI. (2020). *Annual Internet Crime Report*. Retrieved from http\\www.ic3.gov
Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology, 2*(1), 13-20.
Groshkova, T., Stoian, T., Cunningham, A., Griffiths, P., Singleton, N., & Sedefov, R. (2020). Will the current COVID-19 pandemic impact on long-term cannabis buying practices? *Journal of Addiction Medicine*. Advance online publication. https://doi.org/10.1097/ADM.0000000000000724
García-Corral, F. J., Cordero-García, J. A., de Pablo-Valenciano, J., & Uribe-Toril, J. (2022). A bibliometric review of cryptocurrencies: How have they grown? *Financial Innovation, 8*(1), 1–31.
Gupta, A., Maynard, S. B., & Ahmad, A. (2021). The Darkweb phenomenon: A review and research agenda. *arXiv preprint arXiv:2104.07138.*
Groshkova, T., Stoian, T., Cunningham, A., Griffiths, P., Singleton, N., & Sedefov, R. (2020). Will the current COVID-19 pandemic impact on long-term cannabis buying practices? *Journal of Addiction Medicine.*10(5),100-112.
García-Corral, F. J., Cordero-García, J. A., de Pablo-Valenciano, J., & Uribe-Toril, J. (2022). A bibliometric review of cryptocurrencies: How have they grown? *Financial Innovation, 8*(1), 1–31. https://doi.org/10.1186/s40854-022-00317-7
Hadlington, L., & Chivers, S. (2018). Law enforcement awareness of cyber threats. *Computers in Human Behavior, 88*, 283-289.
HMIC. (2015). *Digital readiness: A review of cybercrime policing strategies*. Retrieved from [URL Placeholder]
Holt, T. J., & Bossler, A. M. (2015). *Cybercrime prevention: The role of law enforcement*. Oxford University Press.
Harrison, J. R., Roberts, D. L., & Hernandez-Castro, J. (2016). Assessing the extent and nature of wildlife trade on the Darkweb. *Conservation Biology, 30*(4), 900–904.
Holt, T. J., & Lampke, E. (2019). The evolution of darknet markets and their impact on cyber policing. *Journal of Criminal Justice, 65*, 101-115.
INTERPOL. (2021). *Cybercrime and law enforcement responses*. Retrieved from https://www.interpol.int/en/content/download/16917/file/ga-2021-89-res-11%20-%20tackling%20global%20cybercrime%20threats%20through%20interpol%20channels.pdf

Jalal, R. N. U. D., Alon, I., & Paltrinieri, A. (2021). A bibliometric review of cryptocurrencies as a financial asset. *Technology Analysis & Strategic Management,*7(5)p.1–16.

Jalal, R. N. U. D., Alon, I., & Paltrinieri, A. (2021). A bibliometric review of cryptocurrencies as a financial asset. *Technology Analysis & Strategic Management*. Advance online publication. https://doi.org/10.1080/09537325.2021.1903493

Krebs, B. (2014). *Spam Nation: The inside story of organized cybercrime*. Sourcebooks, Inc.

Levi, M., & Williams, M. (2013). Cybercrime and social networks: Policing implications. *Criminology & Criminal Justice Journal, 13*(4), 481-497.

Moore, T., & Clayton, R. (2008). The consequences of non-cooperation in the fight against phishing. *The Second APWG eCrime Researchers Summit, 17*(2), 1-15.

Munksgaard, R., & Demant, J. J. (2016). Mixing politics and crime: The role of dark web marketplaces in drug distribution. *International Journal of Drug Policy, 35*, 70-77

Khan, M. A., Pattnaik, D., Ashraf, R., Ali, I., Kumar, S., & Donthu, N. (2021). Value of special issues in the *Journal of Business Research*: A bibliometric analysis. *Journal of Business Research, 125,* 295–313. https://doi.org/10.1016/j.jbusres.2020.12.015

Luong, H. T. (2023). Preliminary findings of the trends and patterns of darknet-related criminals in the last decade. *Security Journal. 5(1) p.110-115.*

Lee, J., & McGuire, M. (2019). Cyber policing preparedness in modern contexts. *Journal of Cyber Policy, 4*(1), 45-68.

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., & Stewart, L. A. (2015). Preferred reporting items for systematic review and meta-analysis protocols (PRISMA-P) 2015 statement. *Systematic Reviews, 4*(1), 1–9.

Manolache, A., Brad, F., Barbalau, A., Ionescu, R. T., & Popescu, M. (2022). VeriDark: A large-scale benchmark for authorship verification on the Darkweb. *arXiv preprint arXiv:2207.03477*

Nazah, S., Huda, S., Abawajy, J., & Hassan, M. M. (2020). Evolution of Darkweb threat analysis and detection: A systematic approach. *IEEE Access, 8,* p.171796–171819.

Nunes, E., Diab, A., Gunn, A., Marin, E., Mishra, V., Paliath, V., & Shakarian, P. (2016). Darknet and deepnet mining for proactive cybersecurity threat intelligence. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 7–12).

NCA. (2020). *National crime statistics and the dark web*. Retrieved from https://www.cliffordchance.com/insights/resources/blogs/talking-tech/en/articles/2020/03/national-crime-agency-sets-out-plans.html

Office for National Statistics (ONS). (2019b). Cybercrime reporting in the UK. Retrieved from http\\www.crimestatistics@ons.gov.uk

Orsolini, L., Papanti, D., Corkery, J., & Schifano, F. (2017). An insight into the deep web: Why it matters for addiction psychiatry? *Human Psychopharmacology: Clinical and Experimental, 32*(3), p.2573.

Rai, S., Singh, K., & Varma, A. K. (2020). A bibliometric analysis of deep web research during 1997-2019. *DESIDOC Journal of Library & Information Technology, 40*(2).

Rawat, R., Mahor, V., Chouhan, M., Pachlasiya, K., Telang, S., & Garg, B. (2022). Systematic literature review (SLR) on social media and the digital transformation of drug trafficking on Darkweb. In *International Conference on Network Security and Blockchain Technology* (pp. 181–205). Springer.

Rai, S., Singh, K., & Varma, A. K. (2020). A bibliometric analysis of deep web research during 1997–2019. *DESIDOC Journal of Library & Information Technology, 40*(2), 102–110. https://doi.org/10.14429/djlit.40.02.15008

Raman, R., Achuthan, K., Nair, V. K., & Nedungadi, P. (2022). Virtual laboratories: A historical review and bibliometric analysis of the past three decades. *Education and Information Technologies, 27*(8), 11055–11087.

Riek, M., Böhme, R., & Moore, T. (2016). Understanding the influence of cybercrime on victim reporting behavior. *Computers & Security, 59*, 20-34.

Sonmez, E. D. A., & Codal, K. S. (2022). Terrorism in cyberspace: A critical review of Darkweb studies under the terrorism landscape. *Sakarya University Journal of Computer and Information Sciences,8(1) p.5*

She, Y., Xu, D., Tan, Z., & Zhao, J. (2022). Research hotspot and trend analysis of anonymous communication based on Citespace. In *2022 3rd International Conference on Information Science, Parallel and Distributed Systems (ISPDS)* (pp. 58–62). IEEE.

Sirola, A., Nuckols, J., Nyrhinen, J., & Wilska, T. A. (2022). The use of the Darkweb as a COVID-19 information source: A three-country study. *Technology in Society, 102012.*

Tavabi, N., Bartley, N., Abeliuk, A., Soni, S., Ferrara, E., & Lerman, K. (2019). Characterizing activity on the deep and Darkweb. In *Companion Proceedings of the 2019 World Wide Web Conference* (pp. 206–213).

Tazi, F., Shrestha, S., De La Cruz, J., & Das, S. (2022). SoK: An evaluation of the secure end-user experience on the Darknet through systematic literature review. *Journal of Cybersecurity and Privacy, 2*(2), 329–357.

UNODC. (2021). *The impact of cryptocurrency on transnational crime*. Retrieved from [URL Placeholder]

Verma, S., & Gustafsson, A. (2020). Investigating the emerging COVID-19 research trends in the field of business and management: A bibliometric analysis approach. *Journal of Business Research, 118,* 253–261. https://doi.org/10.1016/j.jbusres.2020.06.057

Van de Weijer, S., Leukfeldt, R., & Holt, T. (2019). Victimology in cybercrime. *International Journal of Cybersecurity, 7*(3), 101-117.

Yar, M., & Steinmetz, K. (2019). The complexities of prosecuting cybercrime.

Theoretical Criminology, 23(2), 173-188.
Zetter, K. (2015). *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. Crown